2010-2016 CAPITAL PLAN
PROPOSED CAPITAL PROJECT
FORM SYP-P2
PLAN VERSION - 3
7/30/2009

Branch:	Executive Branch
Cabinet/Function:	Finance and Administration Cabinet
Agency/Institution:	Commonwealth Office of Technology

Project Title	Enterprise Cyber Security and Identity Managemen
Category	Information Technology System
Biennium	2014-2016
Location (county)	Multi-County
Location (ADD)	N/A
Appropriation Unit	0790

Additional Funding? No

Brief Description/Justification:
The security of Kentucky's computing and networking environments is growing in complexity to the point that it is becoming impossible to manage without automated tools. Hackers are becoming far more sophisticated in their cyber attacks and exploits; more users need access to a larger number of IT resources; computing platforms are increasingly complex and heterogeneous; and Web services are driving the need to manage transactions, as well as citizen and employee access to IT resources. As federal Homeland Security moves to strengthen the nation's cyber security defenses, Kentucky must also fortify its cyber security defenses to ensure that the Commonwealth is prepared for future cyber attacks currently under development.

Commonly used directories and platform-specific security administration tools are not capable of addressing the comprehensive cyber security requirements of a large enterprise like Kentucky State Government. A range of other technologies, including user provisioning, single sign-on, role management, access management, password management, web access management, data encryption, security information/event management and threat/vulnerability management are needed to provide a comprehensive cyber security solution. No single tool does everything across all platforms and for all application types. A multiproduct Enterprise Cyber Security and Identity Management implementation is the only way to meet these critical enterprise security requirements in an efficient and effective manner.

PROJECT BUDGET

Fund Sources	Amount	Cost Elements	Amount
General Fund		Hardware	250,000
Restricted Funds	3,000,000	Software	750,000
Federal Funds		Professional Services	2,000,000
Road Fund		Digital Data Products	
Agency Bonds		Other(specify)	
Other(Private - Cash)			
Other(LT Financing)			
Total	3,000,000	Total	3,000,000

Explanation of Project Budget
Projections based on in-house estimates.

IMPACT ON OPERATING BUDGET? **Yes**

Explanation of Impact on Operating Budget
COT will need to redirect restricted operational funds to support the operation of this project.

PROJECT DETAIL

Method of Procurement
Program Purpose
Completion Date 06/2012

Existing System? No

Phased Project? Yes
2010 - 2012 Enterprise Cyber Security and Identity Management
2012 - 2014 Enterprise Cyber Security and Identity Management
2014 - 2016 Enterprise Cyber Security and Identity Management

Additional Description/Justification
This initiative aligns completely with the Commonwealth's key programs because it will significantly strengthen the state's computing and network infrastructure, making it more safe, secure, reliable and less susceptible to performance slowdowns. A secure and reliable IT infrastructure is essential to supporting modern government services, programs and initiatives in a successful manner, avoiding disruptions and degradation of services that could adversely impact public safety, public health, citizen confidence and the state's economy. This project will also significantly improve the efficiency of the state's cyber security efforts which are too reliant on manual and labor-intensive processes.

The business drivers for the establishment of an Enterprise Cyber Security and Identity Management infrastructure include:

- A streamlined and more efficient security management and administration process
- Improved and strengthened cyber security controls for on-line applications and all computing and network environments including mobile devices
- Significantly improved security policy enforcement
- Improved customer service and convenience (single sign-on, self-service, 7/24)
- Reduced operations support (application development, help desk, etc.)
- Lower operational costs for all Commonwealth systems and networks
- Improved security audit compliance

Enterprise Cyber Security and Identity Management addresses six major IT security requirements:

1. Security threat and vulnerability management – Kentucky must continually monitor and manage the risks presented by flaws in software and hardware configurations and the actions of cyber hackers and cyber criminals.

2. Security information and event management – Kentucky must be able to manage the enormous amount of security information and security-related events that occur across the entire IT infrastructure.

3. Authentication – Kentucky must ensure that users are properly identified and that these identities are validated to IT resources.

4. Authorization – State government must ensure that users can only access what their job function allows them to access within the enterprise.

5. Administration – State agencies need a consistent, government-wide way to administer and manage user access.

6. Audit – State agencies need to ensure that the activities associated with user access are logged for day-to-day monitoring, regulatory and investigative purposes.

Major Enterprise Cyber Security and Identity Management (IM) cost components will include:

- Cyber security and IM software components including, but not limited to, user provisioning, single sign-on, role management, access management, password management, electronic signature management, web access management, data and network encryption, security information and event management, threat and vulnerability management, and network security
- Software license fees
- Software maintenance charges
- Application integration software modules and connectors (Active Directory, mainframe RACF security integration, etc.)
- Consulting and integration services

The resulting contract deliverables will be sufficient to implement, populate and support a long-term, shared-service Enterprise Cyber Security and Identity Management infrastructure in COT.

The Enterprise Cyber Security and Identity Management infrastructure project will be divided into three implementation phases that will ultimately span a period of approximately six years.

Phase I – The first phase of the project is expected to require two years to complete and will initially begin with the development of the overall requirements and objectives of the cyber security and IM implementation. Phase I will be defined in detail to acquire the needed software, hardware and services to address emerging cyber security threats and implement a limited IM infrastructure solution for a selected group of Executive branch employees and at least one Business-to-Government (B2G) or Government-to-Government (G2G) pilot constituent group. This effort will also facilitate the selection of a business partner for the completion of the project and assistance with the procurement of the necessary components of the IM infrastructure. The solution will utilize common off-the-shelf software rather than attempting to develop these components with in-house staff.

Phase II – During the second phase, COT and other state agencies will add remaining state employees and additional components to the new infrastructure and begin to manage the identity and access of all state employees through this single Enterprise Cyber Security and Identity

Management infrastructure. Additional targeted agency business groups will also be migrated to the infrastructure during this phase.

Phase III – In the third phase, businesses and citizens will be provided an opportunity through the Commonwealth's web portal (Kentucky.gov) to maintain a single account with the Commonwealth to access state government applications and systems.

Subsequent years will see additional refinements to ensure the security and efficient management of the IM infrastructure and the provisioning and password synchronization of all IT systems/environments. Usage of the IM facility by state agencies, citizens and the business community will continue to grow.

Previous COT strategic plans described several objectives that focus on providing shared IT solutions and effective e-government. These objectives and the respective relationship to the Identity Management initiative are outlined below:

1. Maintain an effective, stable, shared IT environment - IM provides enhanced cyber security, customer convenience and numerous process improvement opportunities (provisioning, de-provisioning, password synchronization, etc.) for COT and the Commonwealth IT community.

2. Encourage and enable self-service solutions - IM will allow a customer to establish a single Commonwealth account/identity, conduct self-service password management and conveniently access systems and applications across multiple agencies. This over-arching infrastructure will greatly improve the customer experience as they navigate the various systems and services available at Kentucky.gov.

3. Deploy integrated, efficient, multi-agency solutions - An IM infrastructure will provide a single integrated environment that can be used by COT and state agencies to simplify the customer experience and back-end access/processing problems that have been prevalent for years. As more and more on-line services are made available to employees, citizens and businesses, the current stovepipe approach to security will become more cumbersome to manage.

4. Ensure customer trust and protect the security and privacy of individuals conducting government transactions - An IM infrastructure provides a consistent security interface for account establishment, authorization and access. The facility will allow enforcement of security policies, consistent customer identity management and provide a detailed audit trail of systems access activities. If implemented, future security audits should show significant improvement from current audit results.

5. Continue as a national leader in e-Government - IM infrastructure is an important e-government component. The establishment of a single customer account allows advanced portal functionality such as single sign-on and customization.

Previous CAPITAL PLANS? Yes

2008-2014 Enterprise Cyber Security and Identity Managemen

Differences between the current and most recent previous project? Yes

The previous capital projects, while addressing some identity management concerns, were significantly limited in scope compared to this initiative. The previous projects focused entirely on identity management and did not address a number of cyber security issues that are growing in importance, such as threat and vulnerability management, data and network encryption, security information and event management, and network security. In addition, based on an identity management project currently underway in a single cabinet, it has become clear that the funding requested in previous capital projects was insufficient to fund an enterprise-wide solution.

Previous BUDGET REQUESTS? No

Previous BUDGET AUTHORIZATIONS? No